TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

RAPPORT D'EXAMEN PRELIMINAIRE INTERNATIONAL

(article 36 et règle 70 du PCT)

Référence du dossier du déposant ou du mandataire 76.0557 PCT	**POUR SUITE A DONNER**	voir la notification de transmission du rapport d'examen préliminaire international (formulaire PCT/IPEA/416)
Demande internationale n° PCT/FR00/00483	Date du dépot international *(jour/mois/année)* 25/02/2000	Date de priorité *(jour/mois/année)* 26/02/1999
Classification internationale des brevets (CIB) ou à la fois classification nationale et CIB G11B20/00		
Déposant SCHLUMBERGER SYSTEMES SA et al.		

1. Le présent rapport d'examen préliminaire international, établi par l'administaration chargée de l'examen préliminaire international, est transmis au déposant conformément à l'article 36.

2. Ce RAPPORT comprend 6 feuilles, y compris la présente feuille de couverture.

   ☒ Il est accompagné d'ANNEXES, c'est-à-dire de feuilles de la description, des revendications ou des dessins qui ont été modifiées et qui servent de base au présent rapport ou de feuilles contenant des rectifications faites auprès de l'administration chargée de l'examen préliminaire international (voir la règle 70.16 et l'instruction 607 des Instructions administratives du PCT).

   Ces annexes comprennent 6 feuilles.

3. Le présent rapport contient des indications relatives aux points suivants:

   - I ☒ Base du rapport
   - II ☐ Priorité
   - III ☐ Absence de formulation d'opinion quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle
   - IV ☐ Absence d'unité de l'invention
   - V ☒ Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration
   - VI ☐ Certains documents cités
   - VII ☒ Irrégularités dans la demande internationale
   - VIII ☒ Observations relatives à la demande internationale

Date de présentation de la demande d'examen préliminaire internationale	Date d'achèvement du présent rapport
19/06/2000	14.02.2001
Nom et adresse postale de l'administration chargée de l'examen préliminaire international: Office européen des brevets D-80298 Munich Tél. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Fonctionnaire autorisé Heusler, N N° de téléphone +49 89 2399 2359

Formulaire PCT/IPEA/409 (feuille de couverture) (janvier 1994)

RAPPORT D'EXAMEN PRÉLIMINAIRE INTERNATIONAL

Demande internationale n° PCT/FR00/00483

I. Base du rapport

1. Ce rapport a été rédigé sur la base des éléments ci-après (*les feuilles de remplacement qui ont été remises à l'office récepteur en réponse à une invitation faite conformément à l'article 14 sont considérées dans le présent rapport comme "initialement déposées" et ne sont pas jointes en annexe au rapport puisqu'elles ne contiennent pas de modifications (règles 70.16 et 70.17).*) :

Description, pages:

1,3-15	version initiale			
2,2a	reçue(s) le	24/01/2001	avec la lettre du	22/01/2001

Revendications, N°:

1-19	reçue(s) le	24/01/2001	avec la lettre du	22/01/2001

Dessins, feuilles:

1-8	version initiale

2. En ce qui concerne la **langue**, tous les éléments indiqués ci-dessus étaient à la disposition de l'administration ou lui ont été remis dans la langue dans laquelle la demande internationale a été déposée, sauf indication contraire donnée sous ce point.

   Ces éléments étaient à la disposition de l'administration ou lui ont été remis dans la langue suivante: , qui est :

   ☐ la langue d'une traduction remise aux fins de la recherche internationale (selon la règle 23.1(b)).
   ☐ la langue de publication de la demande internationale (selon la règle 48.3(b)).
   ☐ la langue de la traduction remise aux fins de l'examen préliminaire internationale (selon la règle 55.2 ou 55.3).

3. En ce qui concerne les **séquences de nucléotides ou d'acide aminés** divulguées dans la demande internationale (le cas échéant), l'examen préliminaire internationale a été effectué sur la base du listage des séquences :

   ☐ contenu dans la demande internationale, sous forme écrite.
   ☐ déposé avec la demande internationale, sous forme déchiffrable par ordinateur.
   ☐ remis ultérieurement à l'administration, sous forme écrite.
   ☐ remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.
   ☐ La déclaration, selon laquelle le listage des séquences par écrit et fourni ultérieurement ne va pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.
   ☐ La déclaration, selon laquelle les informations enregistrées sous déchiffrable par ordinateur sont identiques à celles du listages des séquences Présenté par écrit, a été fournie.

4. Les modifications ont entraîné l'annulation :

   ☐ de la description, pages :
   ☐ des revendications, n^{os} :
   ☐ des dessins, feuilles :

5. ☐ Le présent rapport a été formulé abstraction faite (de certaines) des modifications, qui ont été considérées comme allant au-delà de l'exposé de l'invention tel qu'il a été déposé, comme il est indiqué ci-après (règle 70.2(c)) :

   (Toute feuille de remplacement comportant des modifications de cette nature doit être indiquée au point 1 et annexée au présent rapport)

6. Observations complémentaires, le cas échéant :

V. Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

1. Déclaration

Nouveauté	Oui :	Revendications	1-17
	Non :	Revendications	18,19
Activité inventive	Oui :	Revendications	
	Non :	Revendications	1-19
Possibilité d'application industrielle	Oui :	Revendications	1-19
	Non :	Revendications	

2. Citations et explications
   voir feuille séparée

VII. Irrégularités dans la demande internationale

Les irrégularités suivantes, concernant la forme ou le contenu de la demande internationale, ont été constatées :
voir feuille séparée

VIII. Observations relatives à la demande internationale

Les observations suivantes sont faites au sujet de la clarté des revendications, de la description et des dessins et de la question de savoir si les revendications se fondent entièrement sur la description :
voir feuille séparée

Il est fait référence aux documents suivants:

D1: EP - A - 0 849 734
D2: DE - A - 42 42 247
D3: EP - A - 0 774 706
D4: FR - A - 2 643 475
D5: EP - A - 0 809 245

Concernant le point V

Déclaration motivée selon la règle 66.2 (a) (ii) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

1. La présente application **concerne** un disque optique de stockage de données (par exemple, CD à musique).

   De ce fait il se pose le **problème** que ces données peuvent être dupliquées en dépit des droits d'auteurs qui protègent généralement lesdites données. Le problème à résoudre peut donc être vu dans la sécurisation d'un disque optique pour éviter les copies frauduleuses des données contenues dans lesdits disques tout en n'alourdissant par l'utilisation desdits disques. La **solution** proposée dans l'invention est d'utiliser un objet portatif (une puce à circuit intégré) stocké (intégré) dans le disque et permettant de protéger des données du média en les cryptant et d'empêcher ainsi une lecture en clair des données. Une mémoire de l'objet portatif contient un jeu individuel de clefs secrètes. Une copie des données (par exemple, de la musique) est inutilisable puisque lesdites données sont cryptées.

   Selon un premier mode de réalisation de l'invention, auquel les revendications ont été limitées (voir VIII 1.), les données sont envoyées, après avoir été lues du disque, au processeur dans le disque qui les décrypte et qui les renvoie au lecteur sous forme décodée. Le processus de décryptage à lieu dans le module de décryptage intégré dans le disque. La clef secrète reste dans le disque, elle y demeure et elle n'est jamais transmise à l'extérieur.

2. Le **document** D1 décrit un disque optique sécurisé de stockage de données (col. 1, lignes 35-39). Dans ce document, un transpondeur dans la disque émet un signal au lecteur qui permet au lecteur d'accéder à un algorithme de décryptage. Donc la différence entre l'invention telle que définie dans les revendications et D1 est que dans l'invention un crypto processeur dans le disque décrypte les données, tandis que dans D1 le lecteur (en dehors du transpondeur) est responsable au décryptage.

Cependant, il est connu de D4 (voir pages 10, 13 et 14) d'incorporer un crypto processeur dans un disque. Il est évident pour la personne du métier d'appliquer cette caractéristique, avec un effet correspondant, dans un disque suivant le document D1 et d'obtenir ainsi le disque selon la revendication 1.

L'objet de la **revendication 1** (et de la même façon celui de la **revendication 8**) n'impliquent donc pas d'activité inventive (article 33 (3) PCT).

3. Les autres revendications ne définissent que des caractéristiques qui entrent dans la pratique normale d'un homme du métier et qui ne peuvent ainsi prétendre contribuer à une activité inventive.

4. Le lecteur de la **revendication 18** est connu de D1. Les caractéristiques de la revendication 1, à laquelle la revendication 18 fait référence, sont des caractéristiques relatives au disque et donc n'impliquent pas de limitation pour le lecteur qui est l'objet de la revendication 18.

5. La **revendication 19** ne contient pas de caractéristique disant que le processus de décryptage à lieu dans le module de décryptage intégré dans le disque.

Concernant le point VII

Irrégularités dans la demande internationale (règles 5 à 7 PCT)

1. Contrairement à ce qu'exige la règle 5.1 a) ii) PCT, la description n'indique pas l'état de la technique antérieure pertinent exposé dans les documents D2, D3, D4 et D5 et ne cite pas ces documents.

2. Les revendications indépendantes ne sont pas formulées en deux parties.

Concernant le point VIII

Observations relatives à la demande internationale (article 6 PCT)

1. Selon la description, il y a deux modes de réalisation (page 12). Selon le deuxième mode, le lecteur lit la clef secrète du disque, et les données sont décodées dans le lecteur. Ce mode de réalisation de l'invention aussi représenté dans les figures n'est pas couvert par les revendications, parce que le processus de décryptage n'à pas lieu dans le module de décryptage intégré dans le disque. Ce défaut de concordance entre les revendications et la description laisse planer un doute sur l'objet pour lequel une protection est demandée. Ceci entraîne un manque de clarté pour les revendications lorsqu'elles sont interprétées à la lumière de la description (article 6 PCT).

2. Les **revendications 8 et 19**, qui ont sensées définir un procède, contiennent des caractéristiques d'un appareil. La catégorie de ces revendications donc n'est pas claire.

3. Bien que les **revendications 1, 8, 18, 19** aient été rédigées sous forme de revendications indépendantes distinctes, il semble qu'elles aient le même objet et qu'elles ne diffèrent l'une de l'autre que par une variation dans la définition de l'objet pour lequel la protection est demandée et par les termes utilisés pour en définir les caractéristiques. Par conséquent ces revendications ne sont pas concises.

sécurité devient très onéreuse et compliquée puisqu'il faut un nouveau boîtier de sécurité pour tout nouveau média.

Il est possible de protéger un disque optique au moyen d'un transpondeur. Un lecteur du disque est muni d'un interrogateur à radio-fréquence. L'interrogateur émet un signal d'interrogation. En réponse à ce signal, le transpondeur émet un signal de réponse. Ce signal de réponse permet au lecteur d'accéder à un algorithme de décryptage. Le décryptage est effectué dans le lecteur. La demande de brevet européen publiée sous le numéro 0849734 semble décrire une telle protection de disque optique.

Aussi un problème technique à résoudre par l'objet de la présente invention est de proposer un disque optique sécurisé de stockage de données, ainsi qu'un procédé de sécurisation d'un tel disque, qui permettent d'éviter les copies frauduleuses des données contenues dans lesdits disques tout en n'alourdissant pas l'utilisation desdits disques.

Une solution au problème technique posé se caractérise, selon un premier objet de la présente invention, en ce que ledit disque optique comprend un module de décryptage, ledit module comportant :

- une mémoire comprenant au moins une clef secrète ;
- un cryptoprocesseur pour décrypter des données dudit disque à partir de ladite clef ; et
- des moyens d'échange de données permettant d'appliquer les données dudit disque au cryptoprocesseur et de lire des données décryptées du cryptoprocesseur.

Selon la présente invention, un procédé de lecture d'un tel disque optique est remarquable en ce que le procédé comporte les étapes suivantes :

- une étape d'application dans laquelle des données dudit disque sont appliquées au cryptoprocesseur via les moyens d'échange de données,

2a

- une étape de décryptage dans laquelle le cryptoprocesseur décrypte les données dudit disque à partir de ladite clef ; et
- une étape d'extraction dans laquelle des données décryptées sont lues du cryptoprocesseur via les moyens d'échange de données.

Ainsi, comme on le verra en détail plus loin, le dispositif de l'invention permet de protéger des données du média en les cryptant et d'empêcher ainsi une lecture en clair des données. Une copie des données est inutilisable puisque lesdites données sont cryptées. Pour effectuer une lecture desdites données, ces dernières doivent être au

REVENDICATIONS

1 – Disque optique (10) de stockage de données comportant un module (20) de décryptage, ledit module (20) comprenant :

- une mémoire (22) comprenant au moins une clef (K1) secrète ;
- un cryptoprocesseur (21) pour décrypter des données (DATA) dudit disque (10) à partir de ladite clef (K1) ; et
- des moyens d'échange de données, (IN_A, OUT_A, VCC_A, GRD_A) permettant d'appliquer les données (DATA) dudit disque (10) au cryptoprocesseur (21) et de lire des données décryptées du cryptoprocesseur (21).

2 – Disque optique selon la revendication 1, caractérisé en ce que ledit module (20) de décryptage est une puce à circuit intégré.

3 – Disque optique selon la revendication 1, caractérisé en ce que ledit module (20) de décryptage est intégré dans une zone centrale dudit disque (10).

4 - Disque optique selon la revendication 1, caractérisé en ce que les moyens (IN A, OUT_A, VCC_A, GRD_A) d'échange de données sont intégrés au disque (10) au niveau d'une zone centrale.

5 - Disque optique selon la revendication 1, caractérisé en ce qu'il comporte des moyens (E) d'équilibrage permettant d'équilibrer ledit disque.

6 - Disque optique selon la revendication 1, caractérisé en ce que les moyens d'échange de données sont munis de contacts.

7 - Disque optique selon la revendication 1, caractérisé en ce que les moyens d'échange de données sont munis de moyens d'émission d'un champ énergétique.

8 - Procédé de lecture d'un disque optique (10) de stockage de données comportant un module (20) de décryptage ; ledit module (20) comprenant :

- une mémoire (22) comprenant au moins une clef (K1) ;
- un cryptoprocesseur (21) ; et
- des moyens d'échange de données (IN-A, OUT-A, VCC-A, GRD-A),

le procédé comprenant les étapes suivantes :

- une étape d'application dans laquelle des données (DATA) dudit disque (10) sont appliquées au cryptoprocesseur (21) via les moyens d'échange de données (IN-A, OUT-A, VCC-A, GRD-A),
- une étape de décryptage dans laquelle le cryptoprocesseur (21) décrypte les données (DATA) dudit disque (10) à partir de ladite clef (K1) ; et
- une étape de d'extraction dans laquelle des données décryptées sont lues du cryptoprocesseur (21) via les moyens d'échange de données (IN-A, OUT-A, VCC-A, GRD-A).

9 - Procédé selon la revendication 8, caractérisé en ce qu'il comporte une étape supplémentaire selon laquelle :

on modifie préalablement à l'étape de décryptage, les données (DATA) en un format compréhensible par le cryptoprocesseur grâce à une interface cryptoprocesseur (37) comprise dans un lecteur de disque optique.

10 - Procédé selon la revendication 8, caractérisé en ce qu'il comporte une étape supplémentaire selon laquelle :

- on modifie préalablement à l'étape de décryptage, les données (DATA) en un format compréhensible par le cryptoprocesseur grâce à une interface cryptoprocesseur (37) comprise dans un ordinateur (40).

11 - Procédé selon la revendication 8, caractérisé en ce que, dans l'étape de décryptage, les données (DATA) sont décryptées systématiquement, qu'elles soient à l'origine cryptées ou non.

12 - Procédé selon la revendication 8, caractérisé en ce qu'il comporte une étape supplémentaire selon laquelle :

on charge dans un ordinateur (40), un ensemble de données brutes (B) et un ensemble de données décryptées (D) ayant pour même origine un ensemble de données lues dans le disque (10).

13 - Procédé selon la revendication 12, caractérisé en ce que le chargement ce fait de manière alternatif.

14 - Procédé selon la revendication 12, caractérisé en ce qu'un ensemble de données brutes (B) est composé d'au moins une zone de données cryptées inutilisables (Bb), et, un ensemble de données décryptées (D) est composé d'au moins une zone de données décryptées utiles (Da).

15 - Procédé selon la revendication 12, caractérisé en ce qu'un ensemble de données brutes (B) est composé d'au moins une zone de données non cryptées utiles (Ba), et, un ensemble de données décryptées (D) est composé d'au moins une zone de données décryptées inutilisables (Dd).

16 - Procédé selon les revendications 14 ou 15, caractérisé en ce qu'il comporte une étape supplémentaire selon laquelle :

- on exécute une partie de code exécutable compris dans une zone de données utiles comprenant des données d'applications.

17 - Procédé selon la revendication 16, caractérisé en ce qu'il comporte une étape supplémentaire selon laquelle :

- on relie différentes zones de données entre elle, on charge de nouvelles données en mémoire, on reconstitue une zone de données au moyen d'un ensemble de liens compris dans le code exécutable.

18 – Dispositif de lecteur de disque (30, 40) agencé pour lire un disque optique (10) de stockage de données tel que défini dans la revendication 1 le dispositif comprenant une interface (37, 38) pour échanger des données avec le module (20) de décryptage.

19 – Procédé de sécurisation d'un disque optique (10) de stockage de données comportant un module (20) de décryptage, ledit module (20) comprenant :

- une mémoire (22) ;
- un cryptoprocesseur (21) ; et
- des moyens d'échange de données (IN-A, OUT A, VCC A, GRD-A),

le procédé comprenant les étapes suivantes :

- une étape de cryptage dans lequel des données sont cryptées à partir d'au moins une clef (K1) secrète unique afin d'obtenir des données encryptées ;
- une étape d'inscription dans laquelle les données encryptées sont inscrites dans ledit disque optique (10) ; et
- une étape de chargement dans laquelle on charge la clef ou les clefs dans la mémoire (22) du module (20) de décryptage.

Translation 09/914282

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference 76.0557	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/FR00/00483	International filing date (*day/month/year*) 25 February 2000 (25.02.00)	Priority date (*day/month/year*) 26 February 1999 (26.02.99)
International Patent Classification (IPC) or national classification and IPC G11B 20/00, 23/28		
Applicant SCHLUMBERGER SYSTEMES		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 6 sheets, including this cover sheet.

☒ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of 6 sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☒ Certain defects in the international application
- VIII ☒ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
19 June 2000 (19.06.00)	14 February 2001 (14.02.2001)
Name and mailing address of the IPEA/EP Facsimile No.	Authorized officer Telephone No.

Form PCT/IPEA/409 (cover sheet) (January 1994)

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

ernational application No.
PCT/FR00/00483

I. Basis of the report

1. This report has been drawn on the basis of (*Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.*):

☐ the international application as originally filed.

☒ the description, pages 1,3-15, as originally filed,
pages _____, filed with the demand,
pages 2,2a, filed with the letter of 24 January 2001 (24.01.2001),
pages _____, filed with the letter of _____.

☒ the claims, Nos. _____, as originally filed,
Nos. _____, as amended under Article 19,
Nos. _____, filed with the demand,
Nos. 1-19, filed with the letter of 24 January 2001 (24.01.2001),
Nos. _____, filed with the letter of _____.

☒ the drawings, sheets/fig 1-8, as originally filed,
sheets/fig _____, filed with the demand,
sheets/fig _____, filed with the letter of _____,
sheets/fig _____, filed with the letter of _____.

2. The amendments have resulted in the cancellation of:

☐ the description, pages _____
☐ the claims, Nos. _____
☐ the drawings, sheets/fig _____

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

4. Additional observations, if necessary:

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-17	**YES**
	Claims	18, 19	**NO**
Inventive step (IS)	Claims		**YES**
	Claims	1-19	**NO**
Industrial applicability (IA)	Claims	1-19	**YES**
	Claims		**NO**

2. Citations and explanations

Reference is made to the following documents:

D1: EP-A-0 849 734
D2: DE-A-42 42 247
D3: EP-A-0 774 706
D4: FR-A-2 643 475
D5: EP-A-0 809 245.

1. The present application **relates** to an optical disc for storing data (for example, a music CD).

The stated **problem** is that this data can be copied in spite of copyrights which generally protect it. Therefore, the problem to be solved could be considered to be that of securing an optical disc to prevent fraudulent copies being made of the data contained thereon, without making the use of said discs more inconvenient. The **solution** suggested by the invention is to use a portable object (an integrated circuit chip) stored (integrated) in the disc for protecting the media data by encrypting it, thereby preventing the data from being read in the decoded form. A memory of the portable object contains an individual set of secret keys. A copy of

the data (for example, the music) cannot be used since said data is encrypted.

According to a first embodiment of the invention, to which the claims have been restricted (see Box VIII, point 1), once the data has been read from the disc it is sent to the processor in the disc which decrypts said data and sends it to the drive in decoded form. The decryption process takes place in the decryption module built into the disc. The secret key is in the disc and never removed therefrom.

2. **Document** D1 describes a secure optical disc for storing data (Column 1, lines 35-39). In this document, a transponder in the disc transmits a signal to the drive enabling it to access a decryption algorithm. Therefore, the difference between the invention as defined in the claims and D1 is that in the invention a crypto-processor in the disc decrypts the data, whereas in D1 the drive (outside the transponder) carries out the decryption process.

However, it is known from D4 (see pages 10, 13 and 14) to incorporate a crypto-processor in a disc. It is obvious to a person skilled in the art to use this feature, with a corresponding effect, in a disc according to document D1, thus leading to the disc of Claim 1.

Therefore, the subject matter of **Claim 1** (and similarly that of **Claim 8**) does not involve an inventive step (PCT Article 33(3)).

3. The other claims merely define features that form part of standard practice for a person skilled in the art and cannot, therefore, purport to contribute an inventive step to the invention.

4. The drive of **Claim 18** is known from D1. The features of Claim 1, to which Claim 18 refers, are features relating to the disc and do not, therefore, have a limiting effect on the drive forming the subject matter of Claim 18.

5. **Claim 19** does not contain a feature stating that the decryption process takes place in the decryption module built into the disc.

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

1. Contrary to the requirement of PCT Rule 5.1(a)(ii), the relevant prior art disclosed in documents D2, D3, D4 and D5 has not been indicated in the description, nor have these documents been cited.

2. The independent Claims are not written in the two-part form.

VIII. Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

1. According to the description, there are two embodiments (page 12). According to the second embodiment, the drive reads the secret key of the disc, and the data is decoded in the drive. This embodiment of the invention also shown in the figures is not covered by the claims since the decryption process does not take place in the decryption module built into the disc. This inconsistency between the claims and the description casts doubt on the subject matter for which protection is sought, thereby rendering the claims unclear when interpreted in the light of the description (PCT Article 6).

2. **Claims 8 and 19**, which are supposed to define a method, contain apparatus features. Therefore, the category of these claims is unclear.

3. Although **Claims 1, 8, 18 and 19** have been written as separate independent claims, it would appear that they have the same subject matter and only differ by virtue of different definitions of the subject matter for which protection is sought and the terms used to define the features. Therefore, these claims are not concise.